

# OpenSSH HideVersion patch

OpenSSH is one of the greatest thing since sliced bread, thanks to all the developers.

The purpose of this page is

- to show a small patch for OpenSSH which hides the version number from the banner

## Prerequisites

You should have OpenSSH source unpacked and be able to compile it from source. Try compiling before applying the patch then apply it and rebuild - no need to waste time if the pristine sources don't even build :-).

## Goals

Hide the version from OpenSSH sshd banner. Normally the sshd daemon running will provide a banner such as:

```
lund@tyr > telnet localhost 22
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_3.8.1p1
Protocol mismatch.
```

This banner reveals the exact version of the daemon running and will help an attacker to target the system, should an exploit be available. It is true that hiding the version number is security by obscurity - but that is fine. Real security combined with security by obscurity is great, and makes an attacker use up more resources.

## OpenSSH sshd HideVersion patch

The patch was tested on Mac OS X and OpenBSD using OpenSSH 4.5. Really this is just a silly little patch, and I haven't tried submitting it to the developers of OpenSSH, as I expect them to flame me and my asbestos suit is at the firecleaners :-).

I think this feature is worth having and I wish the developers of OpenSSH incorporates something like it someday.

Note: the current FAQ about this issue <http://www.openssh.org/faq.html#2.14> which essentially says that this is necessary for compatibility because the SSH protocol is not finished.

By using this patch you should be on the lookout for any problems, and NOT bug the OpenSSH developers if it doesn't suit your needs - YMMV. None the less I have built my sshd daemons for some years manually with the version number removed and not had any problems, which is why I decided to do a patch.

## Using the new option HideVersion

After applying this patch you have a new option HideVersion which can be yes or no, and the manual page is also updated. The manual page update is this:

HideVersion

Specifies whether sshd(8) should hide the version in the banner to make it less easy to identify current version. The default is ``no".

The option to add to sshd\_config configuration file for OpenSSH is then:

```
HideVersion yes
```

With this option present and with yes the sshd daemon hides the version, but if not present or set to no it will behave as usual. When the option is active the banner will not include the version, but the text HIDDEN where the version used to be:

```
$ telnet localhost 22
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-HIDDEN
Protocol mismatch.
```

If you observe any problems then please send me an e-mail.

## Download the patch from

<http://www.kramse.dk/files/patches/openssh/openssh-hideversion.patch>

## Applying the patch

To apply this patch download the sources for OpenSSH and the patch itself. Then unpack OpenSSH and apply it:

```
$ ls -l
total 1896
-rw-r--r--  1 hlk  hlk  965925 Jan 21 21:28 openssh-4.5p1.tar.gz
-rw-r--r--  1 hlk  hlk   3088 Jan  3 17:04 openssh-hideversion.patch
$ tar xzf openssh-4.5p1.tar.gz
$ cd openssh-4.5p1
$ patch < ../openssh-hideversion.patch
```

## Default Publication

```
patching file servconf.c
Hunk #1 succeeded at 114 (offset 7 lines).
Hunk #2 succeeded at 235 (offset 12 lines).
Hunk #3 succeeded at 290 (offset 25 lines).
Hunk #4 succeeded at 394 (offset 37 lines).
Hunk #5 succeeded at 978 (offset 43 lines).
patching file servconf.h
patching file sshd.c
Hunk #1 succeeded at 418 (offset 17 lines).
patching file sshd_config.5
$ ./configure --prefix=/usr/local --sysconfdir=/etc/
--with-ssl-dir=/usr/local
checking for gcc... gcc
...
$ make
...
$ sudo make install
...
// stop the running sshd and start the newly compiled one
$ ps auxw | grep sshd
root        62      0.0  0.0   29092    300  ??  Ss      3:38PM   0:00.01
/usr/local/sbin/sshd
hlk         12767    0.0  0.0   27780      4  p4  R+      9:37PM   0:00.00
grep sshd
$ sudo kill 62
$ sudo /usr/local/sbin/sshd
$ telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.5
Protocol mismatch.
Connection closed by foreign host.
// shows version from OpenSSH 4.5 since HideVersion is not added to
sshd_config
// now sshd_config was updated and sshd restarted again
$ ps auxw | grep sshd
root         12770    0.0  0.0   29092    324  ??  Ss      9:37PM   0:00.01
/usr/local/sbin/sshd
hlk          12781    0.0  0.0   27780      4  p4  R+      9:38PM   0:00.00
grep sshd
$ sudo kill 12770
$ sudo /usr/local/sbin/sshd
$ telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-HIDDEN
Protocol mismatch.
Connection closed by foreign host.
```

## References

Links to important pages:

- OpenSSH homepage is at <http://www.openssh.org>
- OpenSSH FAQ is at <http://www.openssh.org/faq.html>
- A great page about OpenSSH is Darren Tucker's OpenSSH Page at <http://www.zip.com.au/~dtucker/openssh/>

## Default Publication

Also I would recommend supporting the OpenBSD project responsible for OpenSSH.